CSfC Selections for VPN Gateways

VPN Gateway product-lines used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Protection Profile for Network Devices (NDPP), the NDPP EP VPN Gateway (VPN GW EP), and this validated compliance shall include the selectable requirements contained in this document.

CSfC selections for NDPP evaluations:

FAU_STG_EXT.1.1: The TSF shall be able to [transmit the generated audit data to an external IT entity] using a trusted channel implementing the [IPsec] protocol.

FCS_CKM.1.1: Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")*

FCS_COP.1.1(1): Refinement: The TSF shall perform *[encryption and decryption]* in accordance with a specified cryptographic algorithm *[AES operating in* [CBC, GCM] [assignment: *one or more modes, no other modes])* and cryptographic key sizes 128-bits and 256-bits that meets the following:

- FIPS PUB 197, "Advanced Encryption Standard (AES)"
- NIST SP 800-38A, NIST SP 800-380, [selection :, NIST SP 800-388, NIST SP 800-38C, NIST SP 800-38E, no other standards]

FCS_COP.1.1(2): Refinement: The TSF shall perform cryptographic signature services in accordance with *(3) Elliptic Curve Digital Signature Algorithm (ECDSA} with a key size of 256 bits or greater* that meets the following:

- Case: Elliptic Curve Digital Signature Algorithm
- FIPS PUB 186-3, "Digital Signature Standard"
- The TSF shall implement "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard").

FCS_COP.1.1(3): Refinement: The TSF shall perform *[cryptographic hashing services}* in accordance with a specified cryptographic algorithm [SHA-256, SHA-384] and message digest sizes [256, 384] bits that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

FCS_RBG_EXT.1.2: The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest bit security strength of the keys and hashes that it will generate.

FTP _ITC.1.1: Refinement: The TSF shall use [IPsec] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [selection: authentication server, assignment: [other capabilities]] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP TRP.1.1: Refinement: The TSF shall use [IPsec] provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FCS_IPSEC_EXT.1.1: The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602}, [AES-GCM-128, AESGCM-256 as specified in RFC 4106], and using [selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions); IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.5: The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and *19 (256-bit Random ECP}, 20 {384-bit Random ECP),* [assignment: *other DH groups that are implemented by the TOE, no other DH groups]*.

FCS_IPSEC_EXT.1.6: The TSF shall ensure that all IKE protocols implement Peer Authentication using the *[ECDSA}* algorithm.

CSfC selections for VPN GW EP evaluations:

FCS_COP.1.1(2) Refinement: The TSF shall perform cryptographic signature services in accordance with:
• *Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater] that meets* FIPS PUB 186-3, " Digital Signature Standard" with " NIST curves" P-256, P-384 and [selection: P-521, no other curves) (as defined in FIPS PUB 186-3, " Digital Signature Standard")].

FCS_CKM.1.2 Refinement: The TSF shall generate asymmetric cryptographic keys used for IKE peer authentication in accordance with:
• FIPS PUB 186-3, " Digital Signature Standard (DSS)", Appendix 8.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves];

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECP), and [assignment: other DH groups that are implemented by the TOE, no other DH groups].

FCS_IPSEC_EXT.l.12 The TSF shall ensure that all IKE protocols perform peer authentication using a *[ECDSA]* that use X.509v3 certificates that conform to RFC 4945 and [selection: Pre-shared Keys, no other method].